SONECON

BEYOND PREVENTION: ACCELERATING POST-CYBERATTACK POWER RESTORATION AS A KEY FOR GRID RESILIENCE

Paul Stockton, Sonecon; May, 6th 2016

The electric power industry and its public sector partners are rising to meet a new challenge in cyber resilience. Thus far, their efforts have concentrated on protecting the grid and making it less susceptible to attack. Those efforts are vital and must continue. However, given the increasing severity of the cyber threat, utilities and their partners must also accelerate progress in another dimension of resilience: improving plans, capabilities, and coordination mechanisms to restore power and re-establish the integrity of grid control systems if cyber defenses fail.

This study discusses opportunities to make these improvements. As a starting point, the study examines how utilities restored power so effectively after Superstorm Sandy, and analyzes the problems that utilities confront in building an equivalent restoration system to respond to sophisticated cyber threats. The study also examines the starkly different requests for government support for restoration that might result from a cyber attack. In addition, the study derives lessons learned from Sandy for coordinating such assistance so that it actually serves utility priorities—as opposed to being in the way.

After Sandy, power was restored remarkably quickly because so many utilities across the United States pitched in to help. State and federal agencies aided this flow by responding to industry requests for transportation aircraft and other support capabilities. An equivalent restoration system, tailored to meet the challenges of cyber attacks rather than storms, is essential to build resilience against potential adversaries who are aggressively mapping the US power grid and hiding malware within it.

However, adapting the current restoration system for post-cyber attack operations will entail major challenges. During Sandy, utilities sending assistance to the impact zone were secure in the knowledge that they were safely beyond the reach of the storm. No power company will be beyond harm's way during a nationwide cyber attack. To help restore power when many utility chief executive officers (CEOs) will worry that their companies are next in line for attack, mutual assistance agreements may need to overcome powerful disincentives to provide scarce restoration capabilities. Utilities can leverage exercises such as GridEx to develop specialized agreements and support protocols that can meet these challenges, just as they are doing now for coordinated physical attacks on the grid and other man-made threats.

Differences among the industrial control systems (ICSs) utilities use to manage their operations pose an additional problem. During Sandy, restoration crews arriving from the West Coast could directly contribute to repair efforts of Consolidated Edison and other companies in the stricken region because restringing power lines and other restoration tasks are similar from one utility to the next. Much greater variation exists across ICS software, applications, and system designs. Restoring these operational technology (OT) systems after a cyber attack requires specialized utility-specific training. The electricity sector and its contractors might want to explore cross utility pilot programs to determine how best to overcome these training challenges and whether such programs might be scaled up to help meet regional restoration needs. The sector might also identify which restoration tasks can be performed with less specialized knowledge so that it can focus cyber mutual assistance on providing those functions, allowing more highly trained personnel in a stricken utility to concentrate on ICS remediation.

The utility-specific nature of these OT systems will also limit the ability of government agencies to assist power restoration. State National Guard units offer the most promising potential source of support. Guard personnel performed crucial road clearance and other operations to assist grid repair crews after Sandy. Now, a growing number of State Guard organizations and Department of Defense (DOD) contractors are partnering with their local utilities to train personnel to support post-cyber attack power restoration. These efforts should be evaluated for their cost effectiveness to determine whether they can be expanded nationwide.

Whether US Cyber Command (USCYBERCOM) should be structured to augment this support is less clear. The command has a growing cadre of cyber protection teams with ICS remediation skills. However, these teams' primary focus in an attack will be to protect DOD networks and functions. As occurred during Sandy, the president could direct the DOD to make power restoration a top priority, especially when defense networks remain secure and cyber protection assets are readily available for support missions. Yet, the authorities under which USCYBERCOM would help utilities remediate their OT systems remain uncertain, as do the specific functions that utilities would want USCYBERCOM to perform. Cyber Guard and other exercises could examine and further clarify whether and how USCYBERCOM might assist such power restoration operations.

Restoration after Sandy benefited from a strong foundation to coordinate federal assistance to states and their utilities, undergirded by the *National Response Framework* (NRF). The equivalent document for the cyber realm—the interim *National Cyber Incident Response Plan (2010)*—would almost surely prove inadequate just when the United States needed it most. An especially critical shortfall of the interim plan: it provides state governors with only a minimal role in guiding cyber response efforts, even though state National Guard organizations will likely play an increasingly significant role in supporting power restoration and other response

operations. The core principles of the NRF (including its reliance on governors) should be leveraged to build a new national framework for cyber response, including an effective process for requesting assistance. The cyber response framework should complement and be integrated with other public and private sector initiatives to strengthen power restoration capabilities, especially the playbook initiative led by the Electricity Subsector Coordinating Council (ESCC). The framework should also account for cyber response tasks that go beyond those required for natural hazards, including attributing a cyber attack to those responsible for launching it.

The electricity subsector and its partners should also explore how the grid might be reconstituted once utilities have completed initial power restoration operations in an event. A cyber attack that successfully disrupts subsector functions and services may open the door to changes in the grid architecture that are too technically difficult, expensive, or politically impractical to adopt today. In addition to aggressively accelerating current efforts to strengthen grid resilience, utilities and their partners should begin developing options to reconstitute the post-attack grid before an attack occurs, so that these options will be readily available in the new political and resilience funding environment that a major outage could create.